BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	102 12 656.9
Anmeldetag:	21. März 2002
Anmelder/Inhaber:	SCM Microsystems GmbH, Ismaning/DE
Bezeichnung:	Selective Multimedia Data Encryption
IPC:	H 04 L, H 04 N

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 10. April 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Ebert

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

PRINZ & PARTNER GbR

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS
EUROPEAN TRADEMARK ATTORNEYS

SCM Microsystems GmbH
Oskar-Messter-Str. 13
85737 Ismaning

Unser Zeichen: S 4779 DE
HD

21. März 2002

Selective Multimedia Data Encryption

The present invention relates to a conditional access system wherein digitised multimedia data are transmitted in a continuous transport stream of successive data packets. The invention also relates to a method of producing a partially scrambled or corrupted transport stream from a clear transport stream containing digitised multimedia data in successive data packets.

Data security is an important aspect in multimedia commerce. Conditional access systems (CAS) mainly rely on scrambling of a transport stream containing protected multimedia contents. In Digital Video Broadcast ("DVB"), for example, only subscribers with a conditional access module ("CAM") and a valid subscriber card (Smart Card "SC") can descramble a scrambled transport stream and obtain TV contents in the clear for application to a TV set. The conditional access module must have the capability to process an MPEG stream in real-time at a processing rate of at least about 1.5 MB/sec, thereby placing high demands of performance on the hardware used in the CAM.

The present invention provides a conditional access system for multimedia data that offers acceptable security at drastically reduced requirements on hardware performance. For specific embodiments that include decryption circuitry inside a user smart card, the level of security of such system is even higher than that of conventional ones.

According to the invention, a selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions corresponding to the original positions of the particular data packets in the clear transport stream. Since only selected data packets must be processed for encryption/decryption, the amount of processing is drastically reduced.

According to a specific embodiment of the invention, a selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream, removing and encrypting the particular data packets with an event's encryption key, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the clear transport stream.

The invention uses the fact that in a typical compressed multimedia data stream such as an MPEG stream, the contents of particular data packets are propagated to successive data packets, i.e. successive data packets are dependant on contents of preceding data packets, so that by encrypting only particular data packets, many successive data packets are affected, resulting in a sufficient overall scrambling of the data stream. Given the moderate hardware requirements, decryption can be performed by available Smart Cards, enabling a hardware implementation where the security entirely resides in the Smart Card.

Further, because the key can be changed frequently and a highly effective encryption algorithm such as, for example, DES or 3DES can be used, the security in the proposed system is sufficient for the particular needs. A possibility to enhance security is to use a non public encryption algorithm.

For low value multimedia contents, or in a pay-per-event environment, it will generally be sufficient to send a fixed event decryption key prior to actual transmission of the selectively encrypted transport stream. For higher value multimedia contents, the event decryption key can be changed frequently. In a DVB environment, for example, the event decryption keys can be transmitted with the EMMs (Entitlement Management Message) in the transport stream. A user key available in the user smart card will be used to decrypt in the EMMs, the event decryption keys. Another possibility is to have the event decryption key available in an one-event smart card, that will be sold to users.

In the preferred embodiment of the invention, the event decryption key is transmitted to an authorised receiver provided with a "light" conditional access module. As used here, light means that the conditional access module will not necessarily include hardware or software decryption resources as the decryption may be performed in the user smart card. The selectively encrypted transport stream is transmitted to the receiver. The light conditional access module detects encrypted data packets, removes the encrypted data packets from the received transport stream, decrypts the encrypted data packets with the event decryption key, and inserts the decrypted data packets into the remaining received transport stream at positions corresponding to the respective original positions of the particular data packets within the clear transport stream. Preferably, the encrypted data packets are inserted at positions a predetermined number of data packets ahead of respective original positions.

Further advantages and features of the invention will appear from the following description of preferred embodiments with reference to the drawings. In the drawings:

Figs. 1 to 6 are block diagrams with descriptive legends for different embodiments of a headend equipment for producing selectively encrypted data streams containing digitised multimedia data;

Figs. 7 to 10 are block diagrams with descriptive legends for different embodiments of a user equipment for decoding selectively encrypted data streams containing digitised multimedia data;

Fig. 11 is a diagram illustrating a first embodiment of a method of producing a scrambled or corrupted transport stream from a clear transport stream by selective encryption;

Fig. 12 is a diagram illustrating a method of producing a clear transport stream from a scrambled or corrupted transport stream produced with the method of Fig. 11;

Fig. 13 is a diagram illustrating a second embodiment of a method of producing a scrambled or corrupted transport stream from a clear transport stream by selective encryption; and

Fig. 14 is a diagram illustrating a third embodiment of a method of producing a scrambled or corrupted transport stream from a clear transport stream by selective encryption, wherein the scrambled or corrupted transport stream consists of selectively encrypted packets and DVB scrambled packets.

Claims

1. A conditional access system wherein digitised multimedia data are transmitted in a continuous transport stream of successive data packets, characterised in that a selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the clear transport stream.

2. A conditional access system wherein digitised multimedia data are transmitted in a continuous transport stream of successive data packets, characterised in that a selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions corresponding to the original positions of the particular data packets in the clear transport stream.

3. The system of claim 1 or claim 2, wherein a event decryption key is provided to an authorised receiver provided with the conditional access system, the selectively encrypted transport stream is transmitted to the receiver, the conditional access system detects encrypted data packets, removes the encrypted data packets from the received transport stream, decrypts the encrypted data packets with the event decryption key, and inserts the decrypted data packets into the remaining received transport stream at positions corresponding to the respective original positions of the particular data packets within the clear transport stream.

4. The system of claim 3, wherein the event decryption key is provided on a one-event smart card.

5. The system of claim 3, wherein the event decryption key is provided on a one-limited-period smart card.

6. The system of claim 3, wherein the event decryption key in a DVB environment is transmitted in specific EMMs protected by a user encryption key, the corresponding user decryption key being provided in the CAS, on a user smart card or on a user SIM

7. The system of claims 2 and 3, wherein the conditional access system has a buffer memory to store clear data packets while an encrypted data packet is decrypted.

8. The system of claim 1 or claim 3, wherein said encrypted data packets are inserted at positions a predetermined number of data packets ahead of respective original positions.

9. The system of claim any of claims 3 to 8, wherein said conditional access system includes a chip card with decryption circuitry thereon.

10. The system of claim 9, wherein the chip card is a SIM card.

11. The system of any of the preceding claims, wherein the decryption key is transmitted to a receiver with the selectively encrypted data stream.

12. The system of claim 11, wherein the event decryption key is frequently changed.

13. The system of any of claims 1 to 11, wherein the event decryption key is a fixed key distributed on a pay-per-event basis.

14. The system of claim 13, wherein the event decryption key is transmitted in a GSM network prior to an event and loaded into a SIM or smart card inserted in a SIM or smart card reader of a mobile phone.

15. The system of any of the preceding claims, wherein the event decryption key is provided encrypted with a user encryption key and a corresponding user decryption key is also provided to an authorized user.

16. The system of any of the preceding claims, comprising a headend encoder for producing the selectively encrypted data stream, the headend encoder including a Common Interface CI that in turn has a smart card SC interface for a smart card that has encryption circuitry thereon.

17. The system of any of claims 1 to 15, comprising a headend encoder for producing the selectively encrypted data stream, the headend encoder including a Common Interface CI for a PC card module that has encryption circuitry thereon.

18. The system of any of claims 1 to 15, comprising a headend encoder for producing the selectively encrypted data stream, the headend encoder including a Personal Computer PC with an interface for a chip card containing an event encryption key or a user encryption key, the encryption being processed in the PC.

19. The system of any of claims 1 to 15, comprising a headend encoder for producing the selectively encrypted data stream, the headend encoder including an encoder CI module with a CI&TS (Common Interface and Transport Stream) interface to a professional Set-Top-Box STB.

20. The system of claim 19, wherein the encoder CI module further comprises a high speed interface to a PC, a clear transport stream being sent to the PC via the high speed interface to be selectively encrypted by the PC or by a PC peripheral, said PC peripheral being one of the following

- a smart card reader SCR for a smart card SC having encryption circuitry thereon;

- an encryption PCMCIA module having encryption circuitry and forming a SCR for a headend smart card.

21. The system of any of the preceding claims, wherein said particular data packets are of a nature such that their contents are propagated to successive data packets.

22. The system of any of claims 1 to 20, wherein said particular data packets are data packets containing sign bits of DCT coefficients in an MPEG stream.

23. The system of any of claims 1 to 20, wherein every nth data packet of the transport stream is encrypted, n being a fixed number.

24. The system of any of claims 1 to 20, wherein every nth data packet of the transport stream is encrypted, n being a variable number.

25. The system of claim 24, wherein the variable number n is randomly variable.

26. The system of claim 24, wherein the variable number n is variable as a function of data packet contents.

27. The system of any of claims 3 to 26, wherein the conditional access system is embedded in a user Set-Top-Box STB.

28. The system of any of claims 3 to 26, wherein said conditional access system includes a PC card with a Common Interface CI for connection to a user Set-Top-Box STB.

29. The system of claim 27 or claim 28, wherein said user Set-Top-Box STB is capable of detecting a current encryption level of the transport stream and to direct the transport stream, in accordance with the detected encryption level, to decryption circuitry associated with that encryption level.

30. The system of claim 27 or claim 28, wherein the user Set-Top-Box STB is capable of detecting at least some of the following encryption levels of the transport stream :

- None

- DVB only
- DVB and selective encryption
- Selective encryption only;

and the Set-Top-Box STB is capable of directing the transport stream to at least one of the following decryption means:

- None
- An embedded conditional access system in the Set-Top-Box STB able to cope with DVB only,
- An embedded conditional access system in the Set-Top-Box STB able to cope with selective encryption only,
- An embedded conditional access system in the Set-Top-Box STB able to cope with DVB and with selective encryption,
- A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-Box STB able to cope with DVB only,
- A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-Box STB able to cope with selective encryption only,
- A conditional access module in the 1st Common Interface (CI) slot of the Set-Top-Box STB able to cope with DVB and with selective encryption,
- A conditional access module in the 2nd Common Interface (CI) slot of the Set-Top-Box STB able to cope with DVB only,
- A conditional access module in the 2nd Common Interface (CI) slot of the Set-Top-Box STB able to cope with selective encryption only,

- A conditional access module in the 2nd Common Interface (CI) slot of the Set-Top-Box STB able to cope with DVB and with selective encryption,
- A Smart Card (SC) in a Smart Card Reader (SCR).

31. A method of producing a partially scrambled or corrupted transport stream from a clear transport stream containing digitised multimedia data in successive data packets, characterised in that a selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the clear transport stream.

32. A method of producing a partially scrambled or corrupted transport stream from a clear transport stream containing digitised multimedia data in successive data packets, characterised in that a selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions corresponding to the original positions of the particular data packets in the clear transport stream.

33. A method of producing a scrambled transport stream from a clear transport stream containing digitised multimedia data in successive data packets, characterised in that

- selected data packets are determined within the clear transport stream;
- the selected data packets are processed to obtain control words CW therefrom;

- data packets following each selected data packet are DVB scrambled using control words CW obtained from the preceding selected data packet; and

- the selected data packets are encrypted with an event encryption key.

34. The method of claim 33, wherein the encrypted selected data packets are inserted in the scrambled transport stream at positions ahead in time with respect to the original positions of the selected data packets in the clear transport stream.

Abstract

A conditional access system for multimedia data is disclosed that offers acceptable security at drastically reduced requirements on hardware performance. A selectively encrypted transport stream is formed from a clear transport stream by detecting particular data packets within the clear transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions corresponding to the original positions of the particular data packets in the clear transport stream. For specific embodiments that include decryption circuitry inside a user smart card, the level of security of such system is even higher than that of conventional ones.

Fig 2 : HeadEnd Component : Professional STB, CI module including SCR, encryption by SC

The process is the same as the previous one except that
- encryption is performed in the module or in the headend SC
- selection of packet to be encrypted performed by the µP (software filter) or by a hardware filter.

The Head end component with the PC would be the preferential one as it offers more flexibility.

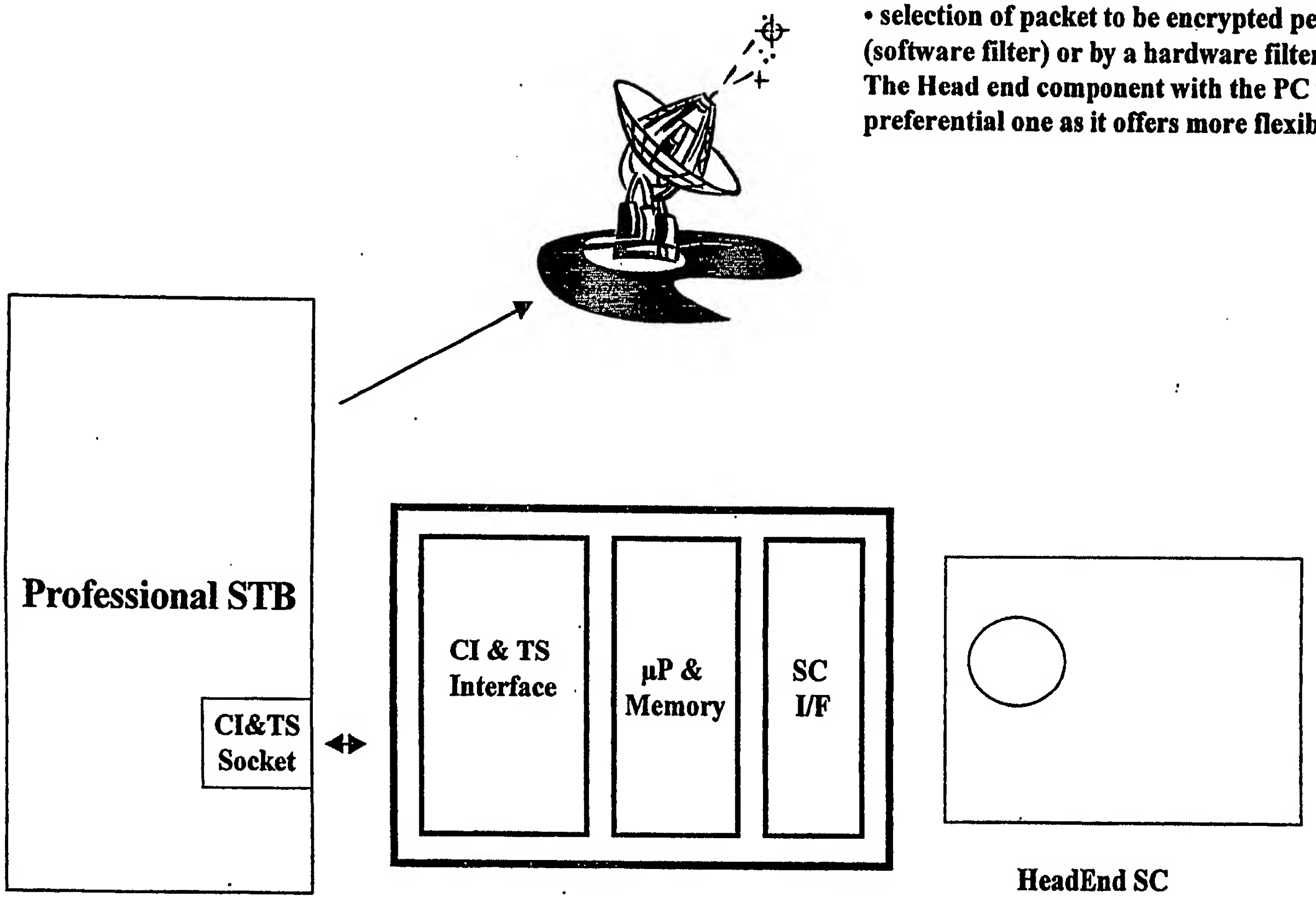


Fig 3 : HeadEnd Component : Professional STB, CI Module including SCR, encryption by Haedend SC

The process is the same as the previous one except that

- encryption is performed in the headend SC
- selection of packet to be encrypted performed by the µP (software filter) or by a hardware filter.

The Head end component with the PC would be the preferential one as it offers more flexibility.

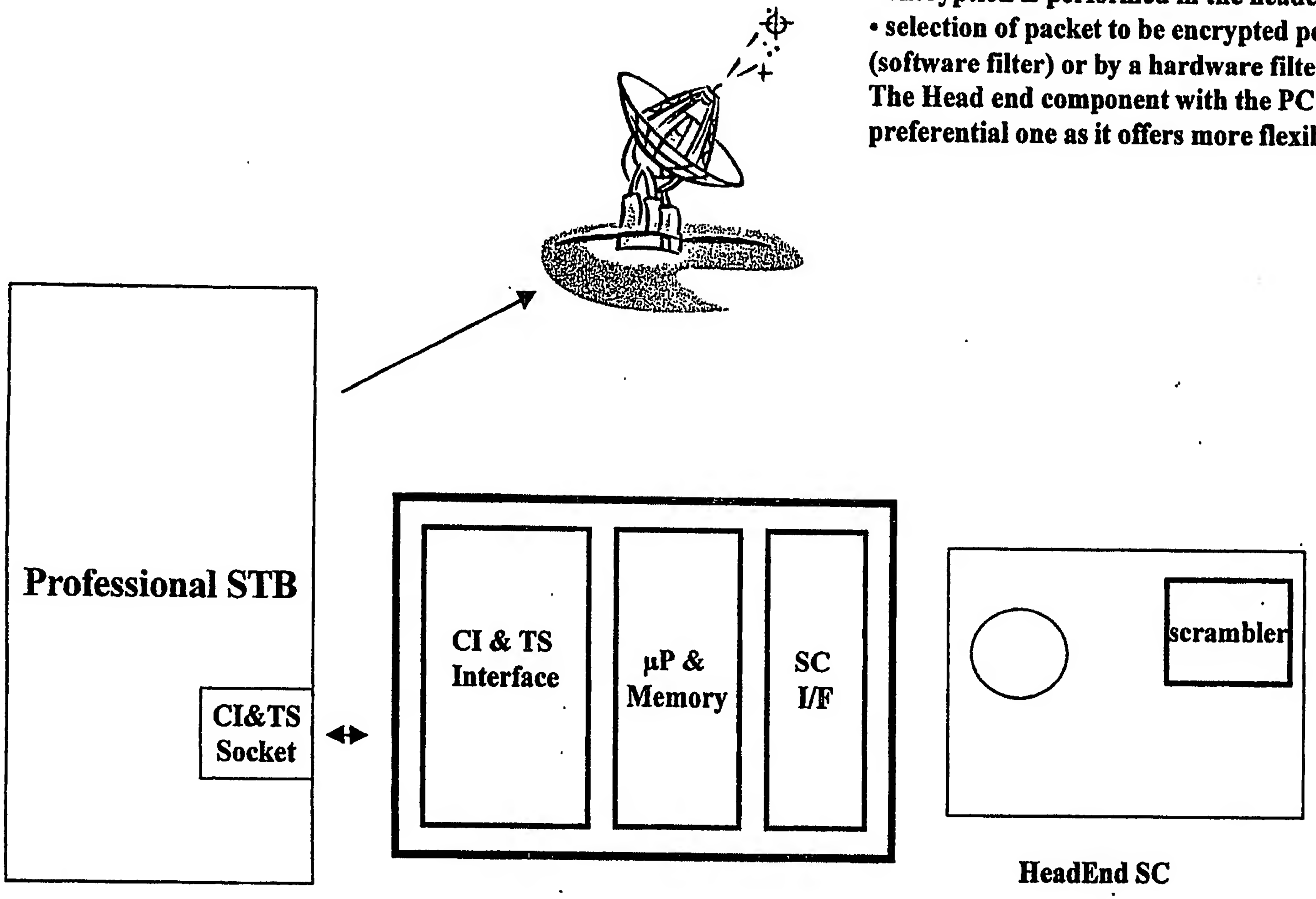
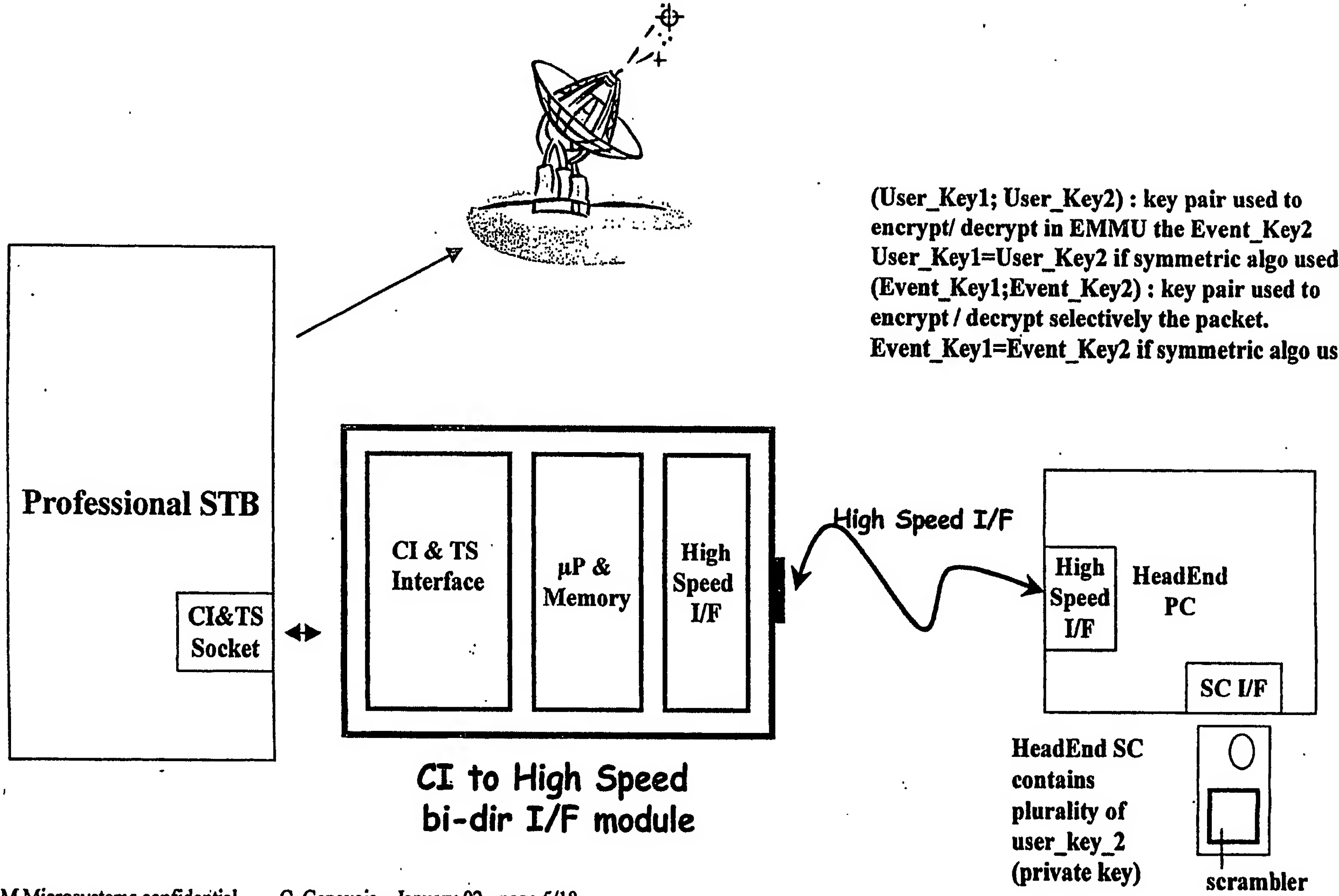


Fig 1 : HeadEnd Compone[illegible]. Professional STB, CI to [illegible] speed bi-directional I/F module and PC with SC I/F and High Speed bi-directional I/F



(User_Key1; User_Key2) : key pair used to encrypt/ decrypt in EMMU the Event_Key2
User_Key1=User_Key2 if symmetric algo used
(Event_Key1;Event_Key2) : key pair used to encrypt / decrypt selectively the packet.
Event_Key1=Event_Key2 if symmetric algo used

Fig 4 : HeadEnd Component : Professional STB, CI module including SCR, encryption by module

The process is the same as the previous one except that
• encryption is performed in the module

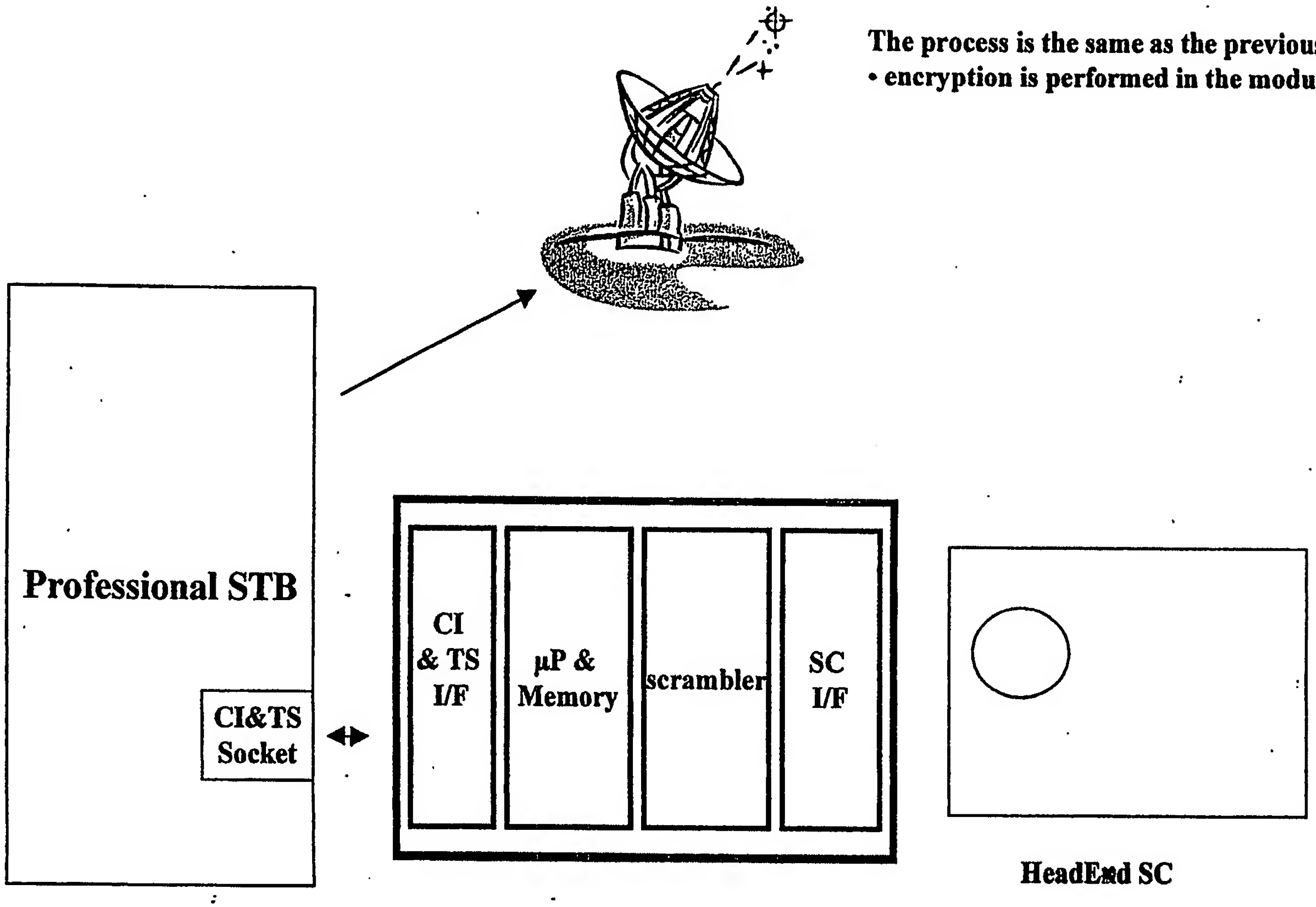


Fig 5 : HeadEnd Component : Professional STB including SCR, encryption by Headend SC

A headend component with a STB including some resources to performed the encryption and a SC interface is a third embodiment of the headend component.

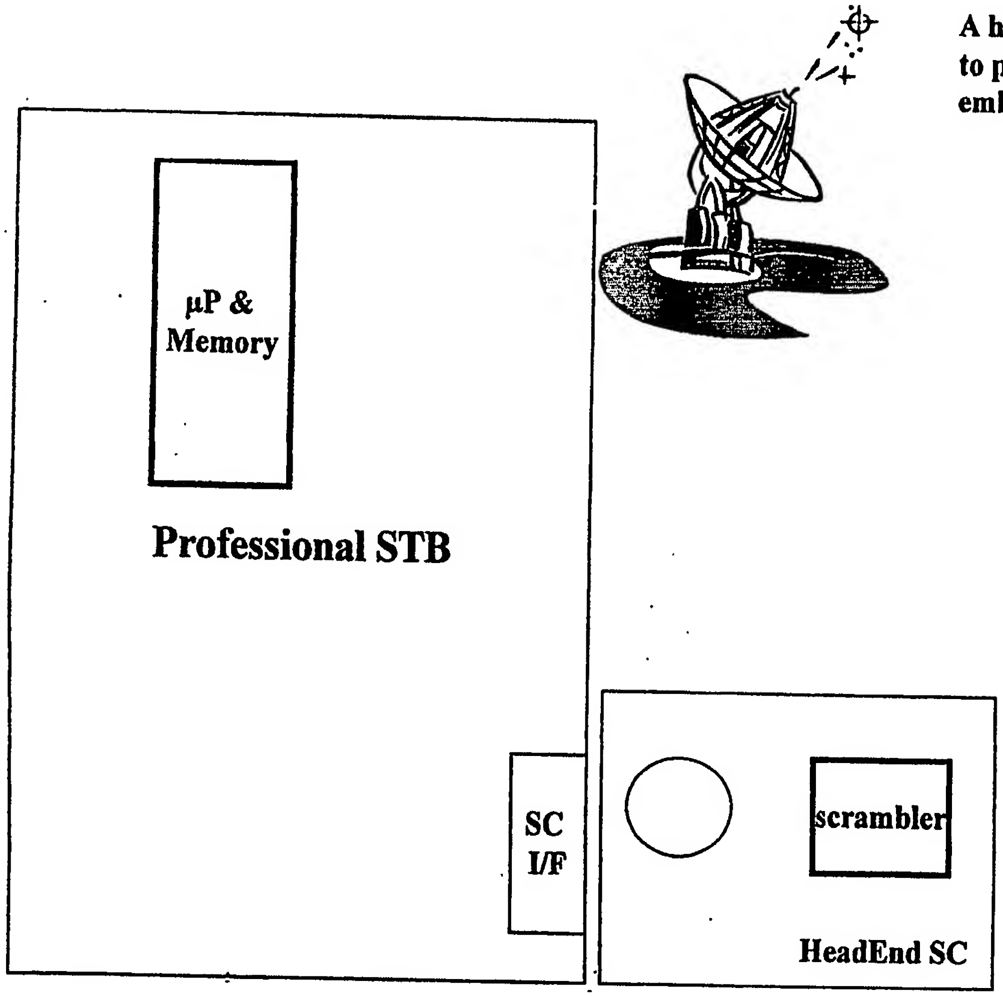


Fig 6 : HeadEnd Component : Professional STB including SCR, encryption by STB

The process is the same as the previous one except that
- encryption is performed in the STB

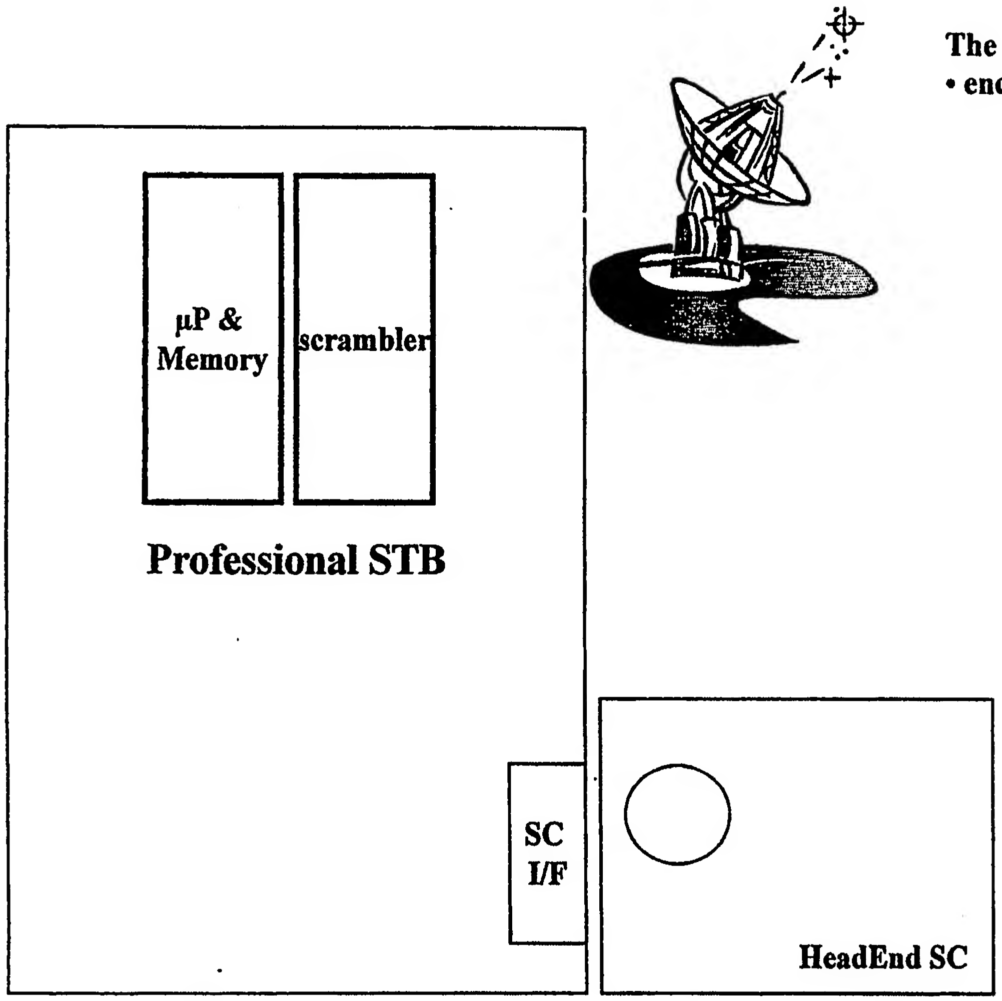


Fig 7 : User decoder : STB + Selective Crypto Module + User SC

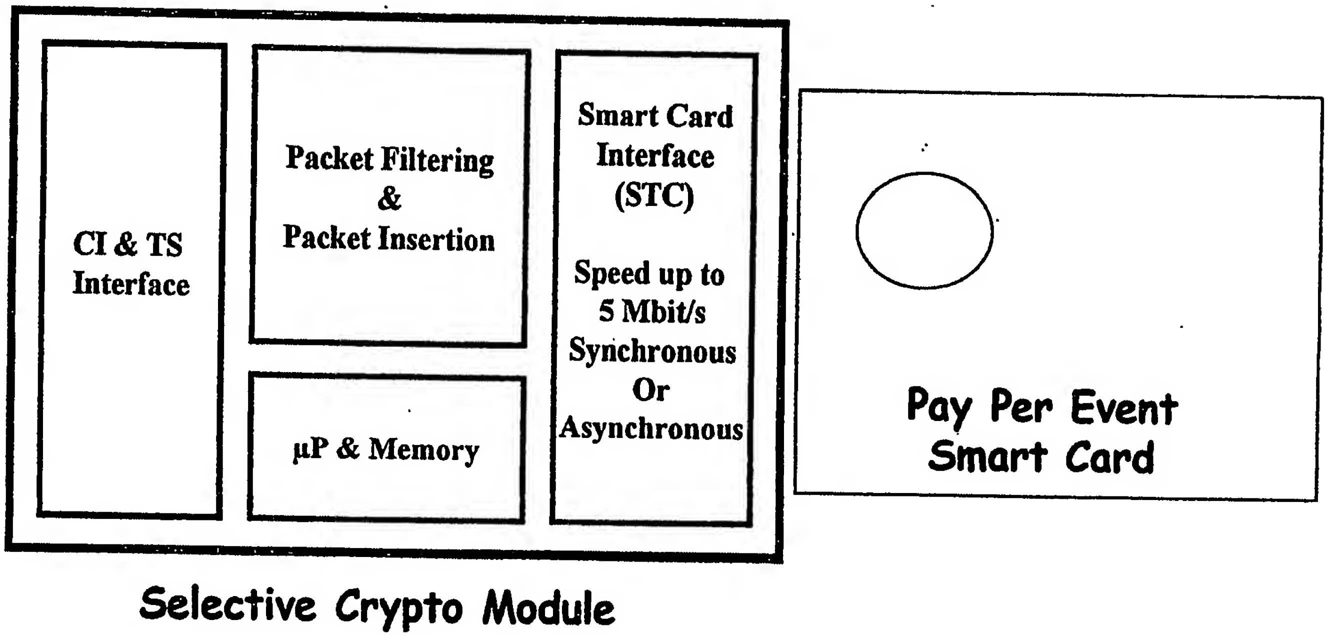
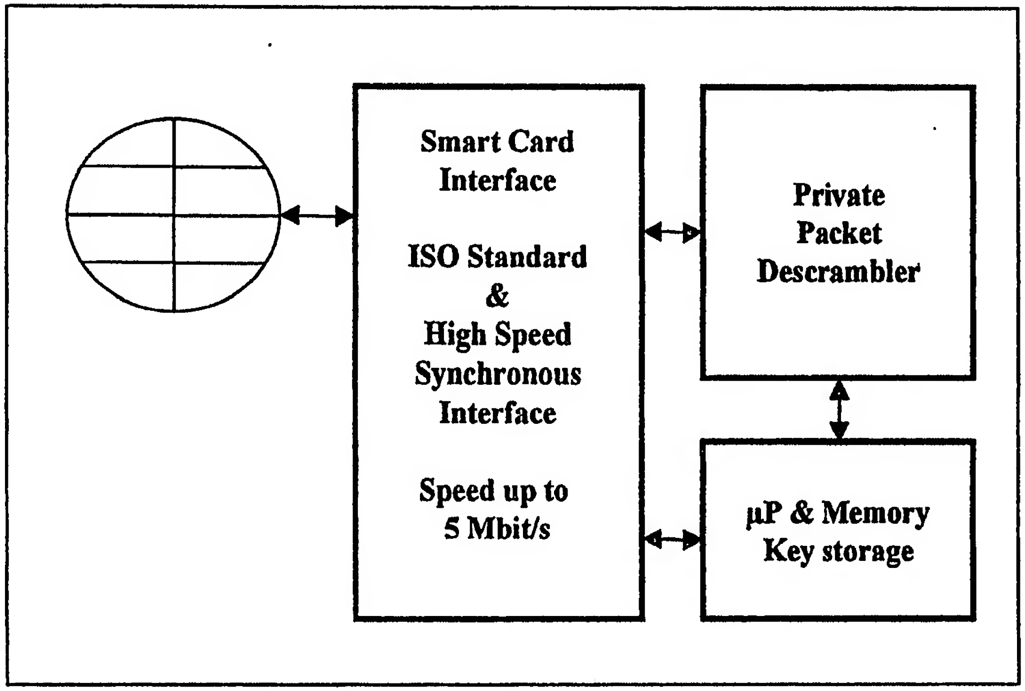


Fig 8 : User SC



Key storage is :
- event_key2 in case that the encryption key is stored in the SC (one event or one period SC)
- user_key2 in case of event_key2 download by using EMMU

Pay Per Event Smart Card

Fig 9 : User decoder : User STB, standard DVB CI updated module and user SC

The process is the same as the previous one except that

- decryption is performed in a standard module updated to be able to cope with standard DVB scrambling and selective encryption
- selective decryption is still performed by the user SC

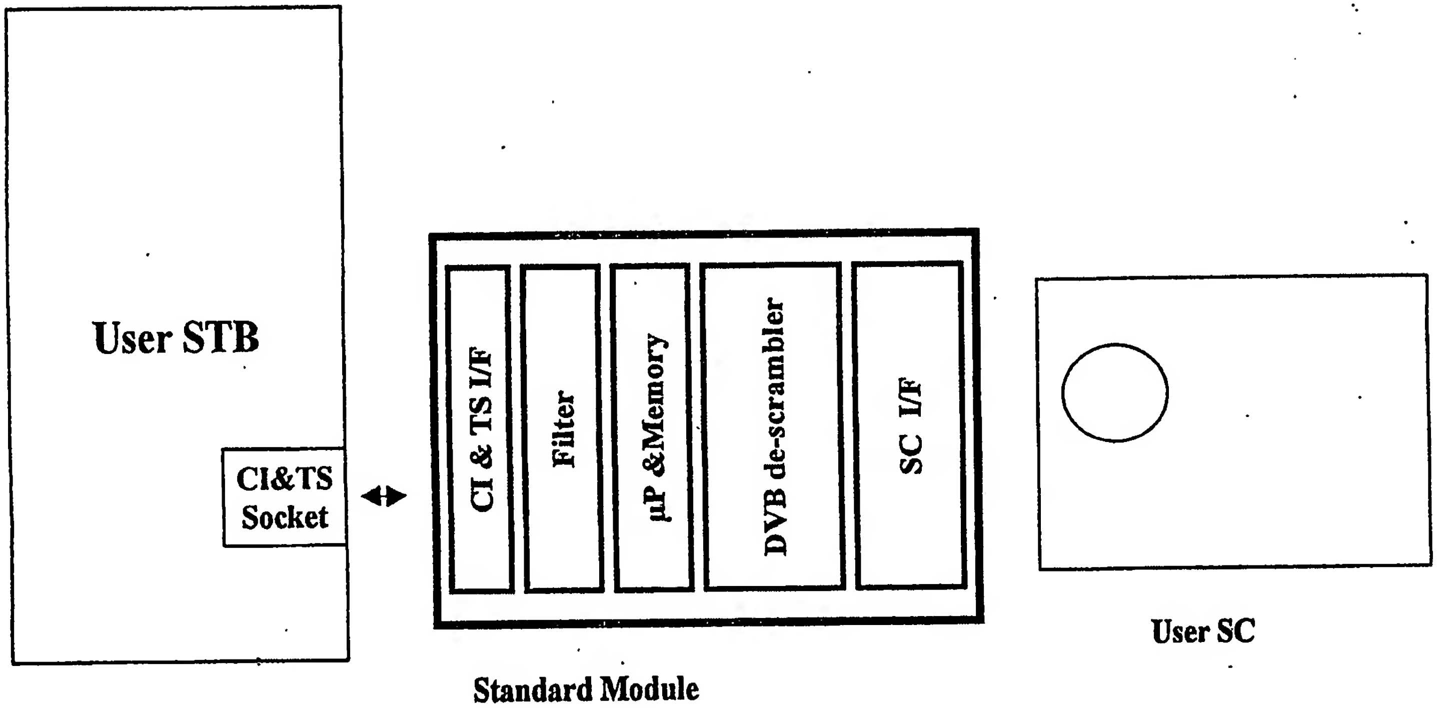


Fig 10 : User decoder : User STB including SCR

The User STB includes some resources to filter the packet and to inserts it properly

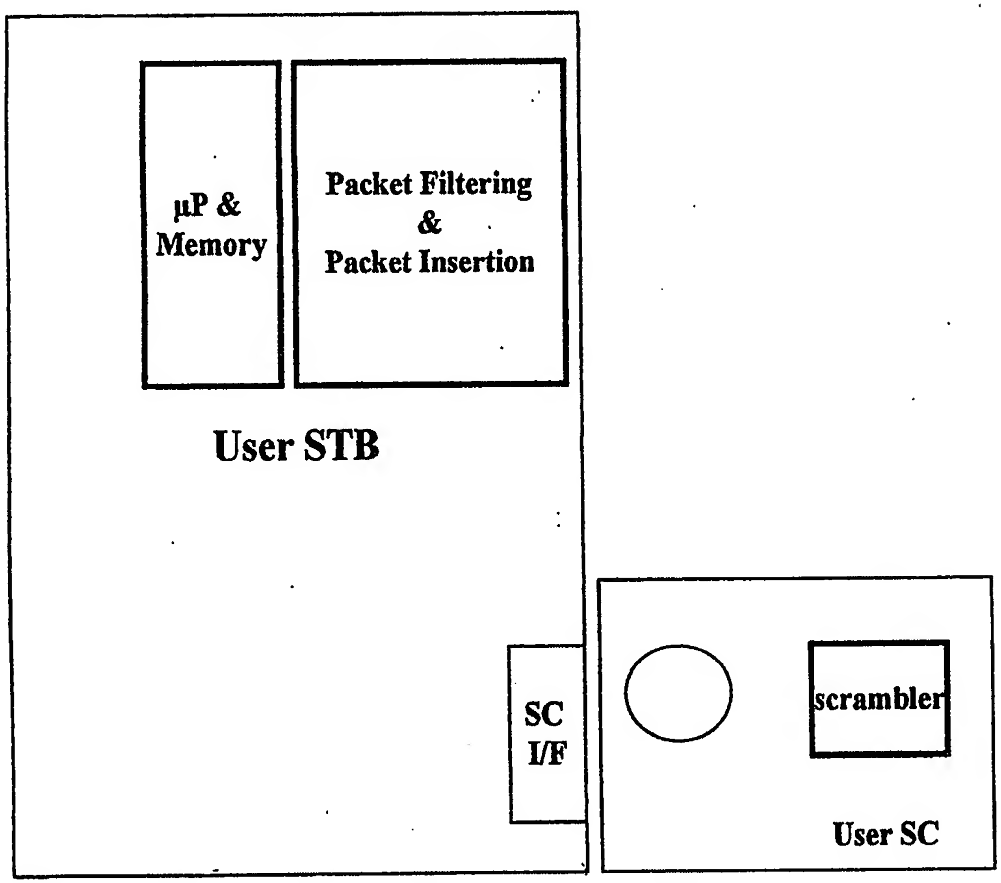


Fig 11 :

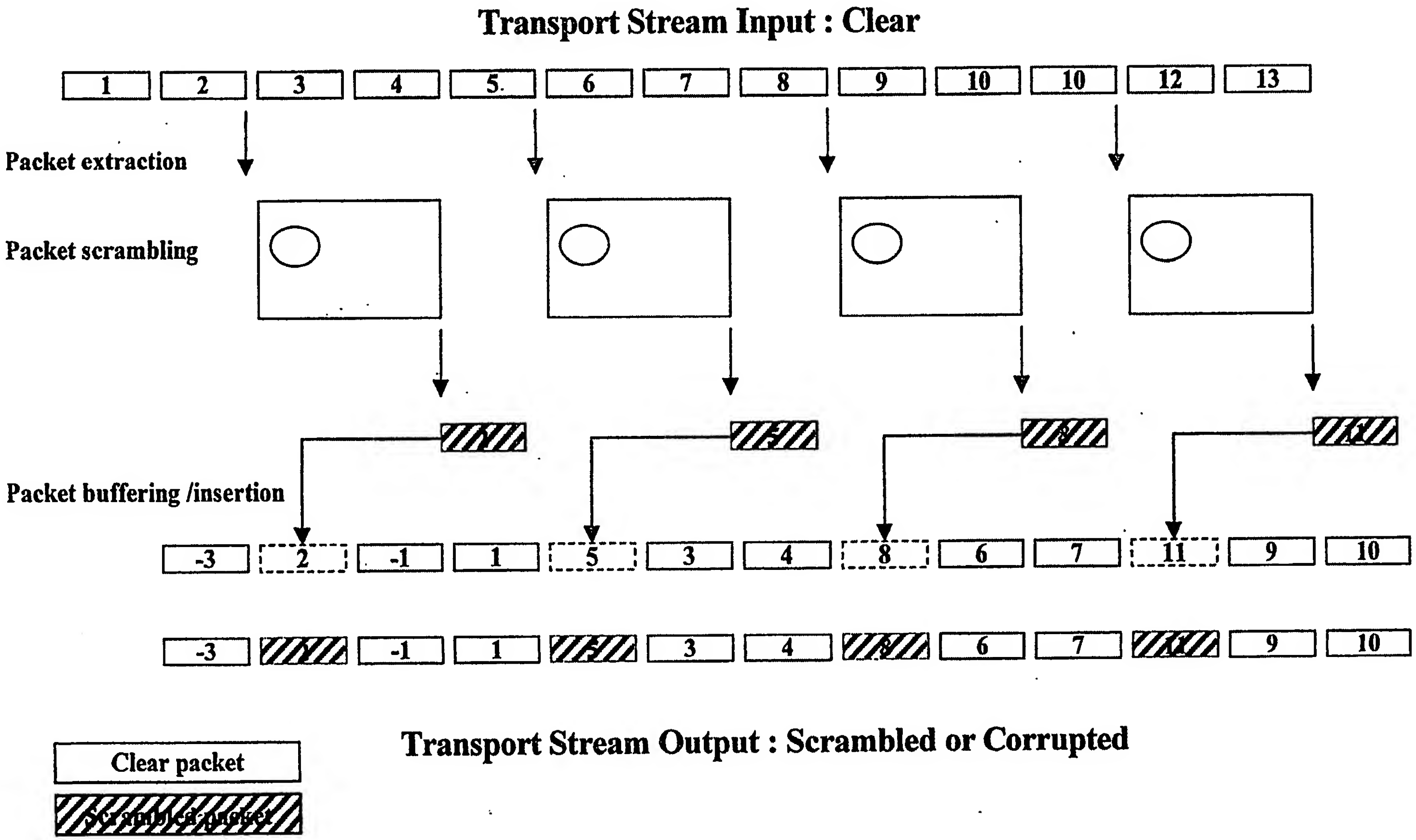

Transport Stream Input : Clear
1
2
3
4
5.
6
7
8
9
10
10
12
13
Packet extraction
Packet scrambling
Packet buffering /insertion
2
5
8
11
-3
2
-1
1
5
3
4
8
6
7
11
9
10
-3
2
-1
1
5
3
4
8
6
7
11
9
10
Transport Stream Output : Scrambled or Corrupted
Clear packet
Scrambled packet

Fig 12 :

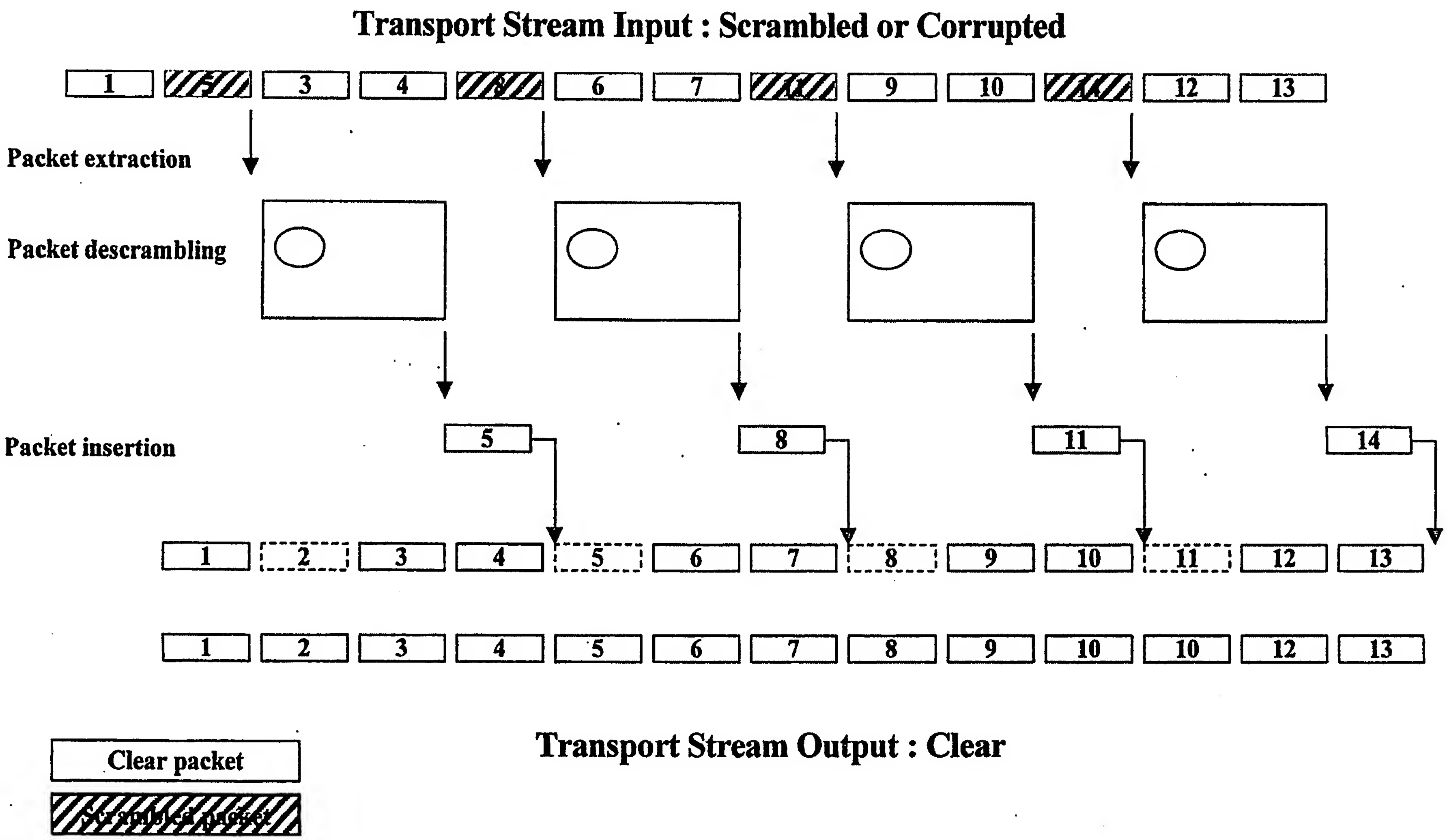
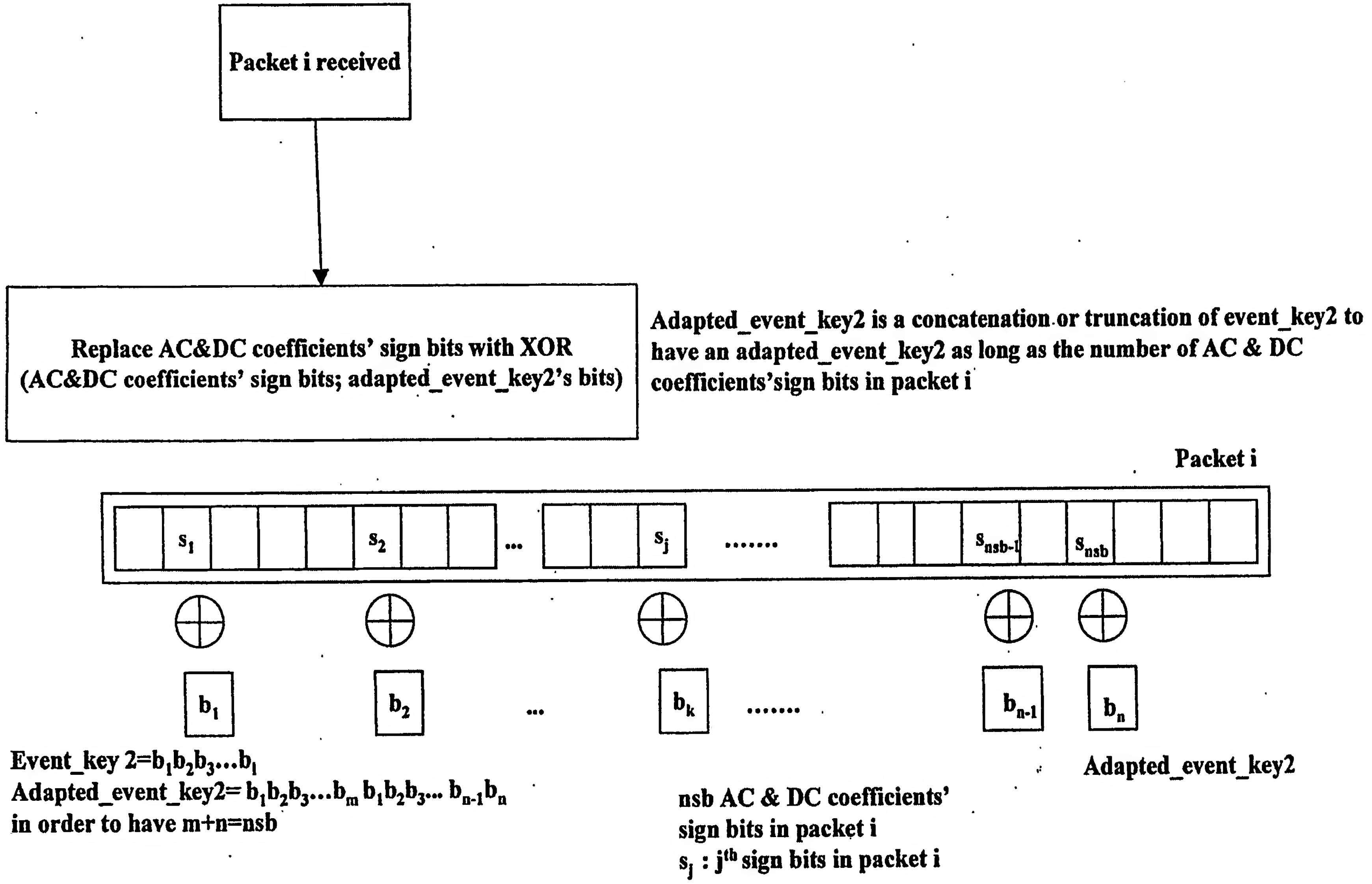

Transport Stream Input : Scrambled or Corrupted
1
3
4
6
7
9
10
12
13
Packet extraction
Packet descrambling
Packet insertion
5
8
11
14
1
2
3
4
5
6
7
8
9
10
11
12
13
1
2
3
4
5
6
7
8
9
10
10
12
13
Transport Stream Output : Clear
Clear packet
Scrambled packet

Fig 13 :AC & DC coefficients' sign bits encryption



Packet i received

Replace AC&DC coefficients' sign bits with XOR (AC&DC coefficients' sign bits; adapted_event_key2's bits)

Adapted_event_key2 is a concatenation or truncation of event_key2 to have an adapted_event_key2 as long as the number of AC & DC coefficients'sign bits in packet i

Event_key 2=$b_1b_2b_3...b_l$
Adapted_event_key2= $b_1b_2b_3...b_m$ $b_1b_2b_3...$ $b_{n-1}b_n$
in order to have m+n=nsb

nsb AC & DC coefficients' sign bits in packet i
s_j : jth sign bits in packet i

Fig 14 :

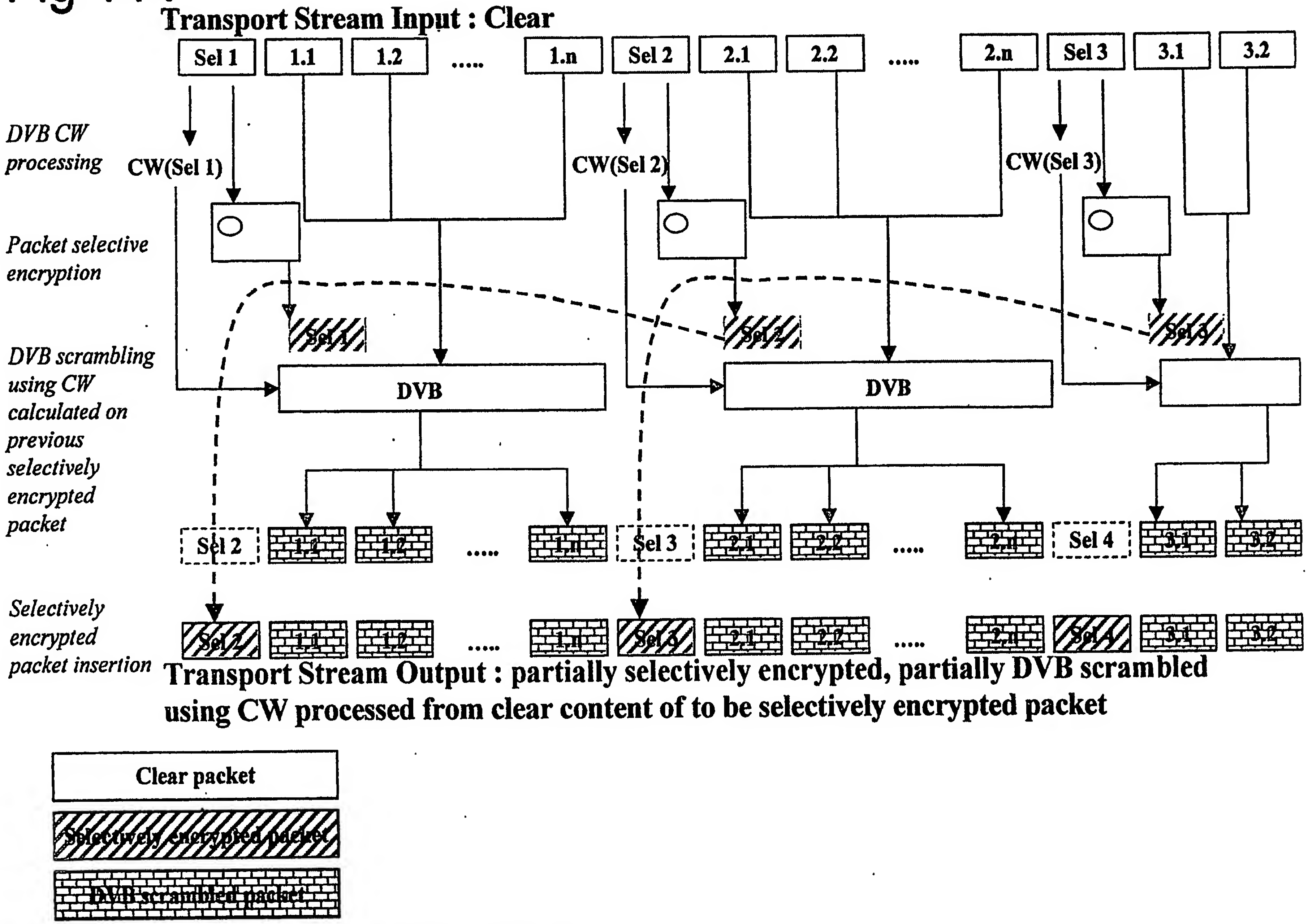

Transport Stream Input : Clear
Sel 1
1.1
1.2
.....
1.n
Sel 2
2.1
2.2
.....
2.n
Sel 3
3.1
3.2
DVB CW processing
CW(Sel 1)
CW(Sel 2)
CW(Sel 3)
Packet selective encryption
Sel 1
Sel 2
Sel 3
DVB scrambling using CW calculated on previous selectively encrypted packet
DVB
DVB
Sel 2
1.1
1.2
.....
1.n
Sel 3
2.1
2.2
.....
2.n
Sel 4
3.1
3.2
Selectively encrypted packet insertion
Sel 2
1.1
1.2
.....
1.n
Sel 3
2.1
2.2
.....
2.n
Sel 4
3.1
3.2
Transport Stream Output : partially selectively encrypted, partially DVB scrambled using CW processed from clear content of to be selectively encrypted packet
Clear packet
Selectively encrypted packet
DVB scrambled packet

Fig 14 : description

A clear content is partially selectively encrypted and partially DVB scrambled, the DVB keys being processed from the clear content of selectively encrypted packet.
By this way, we provide a solution of a stream completely scrambled without using EMM to broadcast DVB keys. The scrambled stream contains the CW that are processed from a selectively encrypted packet that has been decrypted. The level of security is still high as those control words could only be recovered if the "one-event card" is available to decrypt the selectively encrypted packets.
This solution has the advantage that the stream is completely scrambled and that the content's broadcast is independent from EMMs so independent from broadcasting companies (as TPS, Canal + ...etc).

In figure ~~16~~ 14, the process to have the scrambling stream is described :
-to-be-selectively-encrypted packets are sel 1, sel 2, sel 3
-To-be-DVB-scrambled packets are 1.1,1.2,...,1.n,2.1,2.2,...,2.n,3.1, 3.2...
-CW(Sel i) is the control word calculated from clear Sel i content and that will be used to scramble~~d~~ packets i.1,i.2,...,i.n
-As soon as CW(Sel i) is processed, Sel i is encrypted in the head end Smart Card (for example)
-CW(Sel i) is fed to the DVB scrambler to processed the scrambled i.1,i.2,...,i.n
-Encrypted Sel i is inserted in advance to i.1,i.2,...,i.n

When a user STB receives the scrambled stream,
-it will send encrypted packet Sel i to the smart card,
-The smart card will decrypt Sel i,
-The smart card will process CW(Sel i),
-Sel i will be sent to the DVB descrambler,
-The DVB descrambler will descramble packets i.1,i.2,...,i.n with Sel i